The 1998 Amendment to the Roving Wiretap Statute: Congress "Could Have" Done Better

BRYAN R. FALLER*

The roving wiretap statute, 18 U.S.C. § 2518(11)(b) (1994 & Supp. IV 1998), differs from the conventional wiretap statute in that it allows law enforcement officials to follow the suspect from one location to the next, without having to seek court authorization to wiretap each location's telephone line. Congress deemed that such a statute was necessary to combat sophisticated criminals who switched telephones with the purpose of evading wiretap surveillance. The original roving wiretap statute, while arguably intrusive, was constitutional. Although the statute did not comport with the particularity requirement of the Fourth Amendment, it required that before issuance, the court had to find that it was the target's purpose to thwart detection, thus necessitating a roving wiretap. It was this "purpose to thwart" requirement that courts relied on to find the statute constitutional. In 1998, near the end of its session and without ample legislative debate, Congress replaced the "purpose to thwart" requirement with the "could have the effect of thwarting" standard.

This Note argues that the amended version of the roving wiretap statute is unconstitutional because the "could have the effect of thwarting" standard is too easily met and, therefore, will result in general searches. Through an analysis of the history of electronic surveillance, specifically the original roving wiretap statute, this Note explains that the "purpose to thwart" requirement is essential to the roving wiretap statute's constitutionality. Without the "purpose to thwart" requirement, this Note contends, federal law enforcement officials will be able to obtain roving wiretaps based on everyday activities, without a sufficient showing of the necessity for roving surveillance. Accordingly, this Note argues that the amended version of the roving wiretap statute is unconstitutional.

I. INTRODUCTION

> *These requests belong in some bizarre conspiracy novel, not in serious legislative documents being circulated at the top levels of federal law enforcement.*[1]

With the above observation, Representative Bob Barr, a former federal prosecutor and analyst for the CIA, alerted the media of the "wish list" promulgated by the FBI and Department of Justice at the close of the 105th

---

* I would like to thank Professor Sharon L. Davies for her support and inspiration. For their excellent editorial assistance, I would like to give special thanks to Brandy Ritchie, Heidi Reddert, Jeff Wilhelm, and Michael Duffy. Thanks are also due to my parents for their unconditional support. This Note is dedicated to my wife, Elizabeth, who has taught me more than one could ever hope to learn in a classroom.

[1] Robyn Blumner, *Be Careful What You Say: FBI May Be Listening*, CHIC. SUN-TIMES, Nov. 3, 1998, at 29 (statement of Rep. Bob Barr).

Congress.[2] This "wish list" contained, among other items, an amendment to 18 U.S.C. § 2518(11)(b)—the roving wiretap statute.[3] A roving wiretap allows federal law enforcement personnel to place a wiretap on any telephone line from any location that an individual uses.[4] It differs from a conventional wiretap in that a conventional wiretap can be placed only on a specifically designated telephone line at a specific location, which has been specified in the wiretap application.[5] A conventional wiretap allows interception of a particular location's telephone conversations. Thus, if a target switches telephones, the investigators must reapply for a wiretap order for the other phone location. Roving wiretaps, on the other hand, allow investigators to tap any phone that the suspect may use, without having to seek permission for each change of telephone.[6] Furthermore, an application for a conventional wiretap must identify the *location* of the facilities to be wiretapped, whereas a roving wiretap is excused from this requirement.[7]

Prior to the 1998 amendment, law enforcement officials were required to demonstrate that a suspect was "purposely" attempting to evade a conventional wiretap before a roving wiretap could be ordered.[8] However, to the delight of the

---

[2] *See id.*

[3] 18 U.S.C. § 2518(11)(b) (1994), *amended by* Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998). For a description of the changes to § 2518(11)(b), see *infra* Part II.D.2. From this point forward, this Note will use the term "original roving wiretap statute" to refer to the original version of the statute enacted in 1986, and the term "amended roving wiretap statute" to refer to the roving wiretap statute after the 1998 amendment. Changes were made to both § 2518(11)(b) and § 2518(12). Section 2518(12) deals specifically with roving "bugs," not roving wiretaps. *See infra* note 44. The focus of this Note is on § 2518(11)(b) and, hence, it will not mention § 2518(12).

[4] The original version of the roving wiretap statute required that the officer make a probable cause showing that the suspect was purposely trying to evade detection. The 1998 amendment to the roving wiretap statute replaced the "purpose" requirement. *See infra* Part II.D.

[5] *Compare* 18 U.S.C. § 2518(1) (1994) (conventional wiretap statute) *with* 18 U.S.C. § 2518(11)(b) (1994), *amended by* Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998) (roving wiretap statute).

[6] *See* Clifford S. Fishman, *Interception of Communications in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice*, 22 GA. L. REV. 1, 49 (1987) (explaining that authorization to conduct a roving wiretap allows investigators to tap any phone that a suspect uses).

[7] The 1998 amendment does not change this aspect of § 2518(11)(b). Neither the original nor the amended roving wiretap statute requires that the location from where the communications are to be intercepted be disclosed. For a detailed analysis of the purpose for roving wiretaps, see *infra* Part II.B.; *see generally* Fishman, *supra* note 6, at 48–49 (giving a detailed analysis of the birth of the roving wiretap); Michael Goldsmith, *Eavesdropping Reform: The Legality of Roving Surveillance*, 1987 U. ILL. L. REV. 401, 409–11 (1987) (same).

[8] *See* 18 U.S.C. § 2518(11)(b) (1994) (stating that "the applicant makes a showing of a purpose on the part of [the target] to thwart interception by changing facilities").

Clinton Administration and the Department of Justice,[9] the 1998 amendment removed the purpose requirement, thus making it much easier to obtain a roving wiretap.[10] Indeed, the American public should be alarmed with this amendment for two reasons. First, in removing the "purpose" requirement, Congress greatly expanded the scope of an already "intrusive" law.[11] Second, the passage of this amendment, without ample debate, appears particularly dubious.[12]

The 1998 amendment to the roving wiretap statute removed a key mens rea (intent) element from the original roving wiretap statute.[13] The mens rea element that was removed was the "purpose to thwart" requirement. This requirement limited the instances in which a roving wiretap could be ordered. Moreover, the "purpose to thwart" requirement was the leg upon which courts stood to find the

---

[9] Both entities have repeatedly sought to expand the ability to use roving wiretap surveillance. *See generally* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 114 (1997) (explaining that the Justice Department wanted to change the standard to obtain a roving wiretap from an inquiry of the target's intent into an objective inquiry); David B. Kopel & Joseph Olson, *Preventing a Reign of Terror: Civil Liberties Implications of Terrorism Legislation*, 21 OKLA. CITY U. L. REV. 247, 313 n.233 (1996) (explaining that Clinton was a strong supporter of less judicial involvement in the process of obtaining a roving wiretap during the debate of the Antiterrorism and Effective Death Penalty Act of 1996); Timothy Lynch, *Dereliction of Duty: The Constitutional Record of President Clinton*, 27 CAP. U.L. REV. 783, 803–04 (1999) (explaining that Clinton is a supporter of less judicial involvement in wiretap procedures).

[10] *See* Intelligence Authorization Act for 1999, Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998).

[11] *See, e.g.*, Berger v. New York, 388 U.S. 41, 63 (1967) ("Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.") While acknowledging that electronic surveillance is inherently intrusive, this Note also recognizes the strict limitations that are put on electronic surveillance under Title III. *See infra* Part II.A.2. Roving wiretaps, like conventional wiretaps, are intrusive because they enable the government to listen to private conversations. However, with significant limitations placed on the government, the potential for abuse is greatly reduced. The 1998 amendment removes a vital limitation on roving wiretaps and accordingly increases the possibility of abuse.

[12] *See infra* notes 67–88 and accompanying text.

[13] *See* Intelligence Authorization Act for 1999, Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998). Before the 1998 amendment, the roving wiretap statute required that the applicant provide probable cause that the criminal suspect was purposely trying to evade detection. It read in pertinent part: "the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes *a showing of purpose, on the part of that person, to thwart interception by changing facilities*...." 18 U.S.C. § 2518(11)(b)(ii) (1994) (emphasis added), *amended by* Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998). The amended version of § 2518(11)(b)(ii) states: "the application identi[f]ies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is *probable cause to believe that the person's actions could have the effect of thwarting interception* from a specified facility...." 18 U.S.C. § 2518(11)(b) (1994 & Supp. IV 1998) (emphasis added).

original roving wiretap statute constitutional.[14] The 1998 amendment, however, replaced the "purpose to thwart" requirement with the "could have the effect of thwarting" standard.

The roving wiretap statute, as amended, endangers personal privacy; undoubtedly, courts will be forced to decide whether the amended statute is constitutional. Specifically, the courts will have to decide whether the amended statute, which allows a roving wiretap to be issued if a target's actions could have the effect of thwarting conventional wiretap surveillance, violates the particularity requirement of the Fourth Amendment.[15]

This Note argues that the amended roving wiretap statute is unconstitutional because, in eliminating a key mens rea element, the statute now fails to meet the particularity requirement of the Fourth Amendment. In Part II, this Note provides a brief overview of electronic surveillance of communications—from Title III of the Omnibus Crime and Control and Safe Streets Act of 1968 to the adoption of the 1998 amendment. Part III analyzes the "purpose" requirement of the original version of the roving wiretap statute. Part IV explains that the removal of the "purpose" requirement in the amended version of the statute is unconstitutional because it fails to meet the particularity requirement of the Fourth Amendment. Finally, this Note concludes by suggesting that although roving wiretaps are arguably intrusive, they are constitutional when the "purpose to thwart" requirement is an element of the statute.

II. ELECTRONIC SURVEILLANCE OF COMMUNICATIONS: FROM TITLE III TO THE 1998 AMENDMENT[16]

The issues surrounding the electronic surveillance of communications by law enforcement officials have been a steadfast subject of legal debate.[17] Arguably,

---

[14] *See generally* United States v. Gaytan, 74 F.3d 545 (5th Cir. 1996); United States v. Petti, 973 F.2d 1441 (9th Cir. 1992); United States v. Parks, No. 95 CR 510, 1997 WL 136761 (N.D. Ill. Mar. 24, 1997); United States v. Villegas, No. 92 CR 699(CSH), 1993 WL 535013 (S.D.N.Y. Dec. 22, 1993); United States v. Silberman, 732 F. Supp. 1057 (S.D. Cal. 1990), *aff'd*, 973 F.2d 1441 (9th Cir. 1992).

[15] For an explanation of the Fourth Amendment's particularity requirement, see *infra* Part IV.A.

[16] To enable the reader to better understand why the 1998 amendment to the roving wiretap statute is constitutionally questionable, this Note provides an historical description of electronic surveillance law. Sections II.A. and II.B. attempt to educate the reader on the limitations placed upon electronic surveillance. In observing the historical development of electronic surveillance, this Note permits the reader to better understand what roving surveillance is, how it differs from conventional wiretap surveillance, and, most importantly, why the 1998 amendment to the roving wiretap statute stands in stark contrast to the idea of limiting electronic surveillance.

[17] *See, e.g.*, Dempsey, *supra* note 9, at 68 (addressing the privacy issues concerning new communications and computer technologies and the needs of law enforcement); Fishman,

electronic surveillance of communications, no matter what the form, is intrusive.[18] Because of its intrusive nature, Congress has, over the years, promulgated legislation that provides the prerequisites which must be satisfied in order to legally intercept another's communications.[19]

A. *Title III of the Omnibus Crime Control and Safe Streets Act of 1968*

1. Berger v. New York

The Supreme Court addressed, for the first time, how the Fourth Amendment applies to court-ordered electronic surveillance by government officials in the 1967 landmark decision of *Berger v. New York*.[20] In *Berger*, the Court held that New York's eavesdrop statute[21] was "too broad in its sweep," and thus would lead to "general searches" that would violate the Fourth Amendment.[22] The Court

---

supra note 6, at 20–21 (examining the constitutionality of electronic surveillance legislation); Goldsmith, *supra* note 7, at 109–11 (describing roving surveillance).

[18] *See supra* note 11. Electronic surveillance has been considered to be more intrusive than the physical searches and seizures permitted by the Fourth Amendment. *See id.* This is because unlike conventional search warrants, which must identify the area to be searched, electronic surveillance is inherently indiscriminate. *See* Dempsey, *supra* note 9, at 69–70 (explaining that electronic surveillance, such as a wiretap, provides law enforcement officials with "all of the target's communications, whether they are relevant to the investigation" or not). Furthermore, in the execution of a conventional search warrant, an announcement of the authority and purpose is required. This "knock and notice" rule is essential so that a person whose privacy is being invaded can observe the search and seek judicial remedy for any violations. However, electronic surveillance is usually conducted "surreptitiously," without the "knock and notice" of conventional searches. *See id.* at 68.

[19] *See infra* Part II.A.

[20] 388 U.S. 41 (1967); *see also* 1 CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 1:4, at 1-6 (2d ed. 1995) (explaining that Congress enacted Title III in an effort to comport electronic surveillance legislation with the requirements set forth in *Berger*).

[21] N.Y. CRIM. PROC. LAW § 813-a (McKinney 1958), *construed in* Berger v. New York, 388 U.S. 41, 43 n.1 (1967). The statute read in pertinent part:

> An ex parte order for eavesdropping . . . may be issued by any justice of the supreme court or judge . . . upon oath or affirmation of a district attorney, or of the attorney-general or of an officer above the rank of sergeant of any police department of the state . . . that there is reasonable ground to believe that evidence of crime may be thus obtained, and particularly describing the person or persons whose communications . . . are to be overheard or recorded . . . and, in the case of a telegraphic or telephonic communication, identifying the particular telephone number or telegraph line involved.

Id.

[22] *Berger*, 388 U.S. at 43–44. The Court held that although the statute satisfied the Fourth Amendment's requirement of a detached and neutral magistrate, "the broad sweep of the statute

did not hold that electronic surveillance was per se unconstitutional but instead that the New York statute failed to meet the requirements of the Fourth Amendment.[23] In its decision, the Court laid the framework for the constitutional requirements for electronic surveillance.

In *Berger*, the Court outlined seven constitutional requirements for court-ordered electronic surveillance:[24] (1) a probable cause showing that a particular offense has been or is about to be committed; (2) the applicant must describe with particularity the conversations to be intercepted; (3) the surveillance must be for a specific and limited period of time in order to minimize the invasion of privacy; (4) there must be continuing probable cause showings if the surveillance is to continue beyond the original termination date; (5) the surveillance must cease once the conversation sought is seized; (6) notice must be given unless there is an adequate showing of exigency; and (7) a return on the warrant is required so that the court may oversee and limit the use of the intercepted conversations.[25] With such requirements before it, it was not long before Congress enacted a law that followed the *Berger* requirements.

2. *Title III*

"Title III of the Omnibus Crime Control and Safe Streets Act of 1968 empowers law enforcement officials to seek, and judges to issue, court orders authorizing the interception of 'wire communications,' 'oral communications,' and, since 1986, 'electronic communications.'"[26] In promulgating Title III,[27] Congress sought to include the constitutional requirements set forth in *Berger v. New York*[28] and *Katz v. United States*[29] for electronic surveillance.[30] Title III

[was] immediately observable." *Id.* at 54.

[23] Justice Clark, while recognizing that the potential for abuse in electronic surveillance was great, held that it can be within the boundaries of the Fourth Amendment. *See id.* at 62–64. In response to the argument that it would be impossible to draft a warrant or statute to meet the requirements of the Fourth Amendment, Justice Clark noted that "this Court has in the past, under specific conditions and circumstances, sustained the use of eavesdropping devices." *Id.* at 63 (citations omitted).

[24] *See id.* at 58–61. For an analysis of these requirements, see 1 FISHMAN & MCKENNA, *supra* note 20, at 1-6 to 1-7.

[25] *Berger*, 388 U.S. at 58–61; *see also* 1 FISHMAN & MCKENNA, *supra* note 20, at 1-6 to 1-7.

[26] Fishman, *supra* note 6, at 23–24.

[27] *See* Pub. L. No. 90-351, 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510–2522 (1994)).

[28] 388 U.S. 41 (1967). For a listing of these requirements, see text accompanying notes 24–25.

[29] 389 U.S. 347, 355–59 (1967) (reaffirming the requirements for electronic surveillance set forth in *Berger* and holding that a detached and neutral magistrate must determine the scope of the surveillance).

includes several requirements that, while not constitutionally mandated, establish further procedural and substantive prophylactic measures incorporated by Congress.[31] One such example is that, unlike conventional search warrants, which may be issued by a federal magistrate judge, electronic surveillance may be authorized by district or circuit court judges only.[32]

Title III also describes who may authorize a wiretap application, the information that the application must contain, and the requirements that a judge must find before authorizing a wiretap.[33] Other requirements set forth by Title III include the following: how the wiretap is to be executed, what the notice requirements are, and what crimes may be investigated by utilization of a wiretap.[34] One specific requirement in Title III, especially relevant to this Note, is the particularity requirement of the Fourth Amendment.[35] Title III requires that an application for a wiretap be "particular" as to: the particular offense that has been, is being, or is about to be committed; a particular description of the nature and location of the facilities from which, or the place where, the communication is to be intercepted; a particular description of the type of communications sought to be intercepted; and the identity of the suspect if it is known.[36]

---

[30] *See* Fishman, *supra* note 6, at 25 (explaining that Title III was in response to the Supreme Court's decisions in *Berger* and *Katz*).

[31] *See id.* (explaining that Title III does more than "merely parallel the Fourth Amendment and Supreme Court decisions").

[32] *See* 18 U.S.C. § 2510(9)(a) (1994). This Note asserts that because electronic surveillance is inherently more intrusive than searches permitted by a conventional search warrant, this heightened judicial personnel requirement is necessary. For example, issuance of a conventional search warrant results in a fairly quick turnaround—the search is conducted and either contraband is found or it is not. With electronic surveillance, however, the "search" is not so quick. Wiretaps can last up to thirty days, and, under the usual circumstances, the suspect has no idea that his phone is being tapped. This type of prolonged search deserves the attention of a district court or circuit court judge who usually determines if a contested search warrant is constitutional.

[33] *See* 1 FISHMAN & MCKENNA, *supra* note 20, at 1-10 to 1-18 (explaining the requirements of Title III).

[34] For an excellent analysis of the requirements set forth by Title III, see Fishman, *supra* note 6, at 23–35. Professor Fishman gives a detailed explanation and analysis of the requirements of Title III, including relevant legislative history; *see also* JAMES G. CARR, THE LAW OF ELECTRONIC SURVEILLANCE § 2.3, at 2-5 to 2-7 (2d ed. 1987) (detailing the legislative history of Title III); 1 FISHMAN & MCKENNA, *supra* note 20, at 1-10 to 1-18 (explaining the requirements of Title III).

[35] *See infra* Part IV.A. The Fourth Amendment provides in part that "no Warrant shall issue, but upon . . . *particularly describing the place to be searched, and the persons or things to be seized.*" U.S. CONST. amend. IV (emphasis added).

[36] *See* 18 U.S.C. § 2518(1)(b) (1994).

B. *Birth of the Roving Wiretap—The Electronic Communications Privacy Act of 1986*

Roving surveillance is a product of new technologies.[37]

After nearly two decades of relative calm, Title III was amended in 1986 by the Electronic Communications Privacy Act (ECPA)[38] to bring Title III up to date with the technological advances that had occurred during the previous twenty years.[39] With the advent of devices such as cellular telephones, electronic mail, and facsimiles, "the Justice Department, civil libertarians and numerous subdivisions of the telecommunications industry" requested a rewrite of the law, which resulted in the ECPA.[40] As a result of the ECPA, the roving wiretap provision was among the most significant and dramatic amendments to Title III.[41]

The roving wiretap is not a technological advancement. Rather, roving wiretaps employ the same technology as conventional wiretaps. The difference between a conventional wiretap, under Title III, and a roving wiretap, under the ECPA, is statutory in nature: A conventional wiretap application must specify the telephone line to be tapped, but a roving wiretap is expressly excused from this requirement.[42] In other words, an application for a roving wiretap need not specify which telephone an officer wishes to wiretap; instead, the statute permits the officer to wiretap any telephone that the suspect uses.

The necessity of roving surveillance became evident when law enforcement officials noticed that sophisticated criminals began using increased caution to avoid possible wiretaps and other forms of electronic surveillance.[43] In addition,

---

[37] Goldsmith, *supra* note 7, at 409 (explaining that the roving wiretap was "born" to allow federal investigators to place taps on individuals who were utilizing new technologies to evade conventional wiretap surveillance).

[38] Pub. L. No. 99-508, 100 Stat. 1848 (1986). For an exhaustive review of the ECPA, see Fishman, *supra* note 6, at 48–69.

[39] 1 FISHMAN & MCKENNA, *supra* note 20, at 1-18 to 1-19 (explaining that Title III had not kept pace with advances in telecommunications and thus was in dire need of an amendment).

[40] *Id.*

[41] *See* 18 U.S.C. § 2518(11) (1994). For a detailed analysis of the original roving wiretap statute, see Goldsmith, *supra* note 7, at 409–11, 415–25 (explaining the origins and constitutionality of roving surveillance).

[42] *See* 18 U.S.C. § 2518(1)(b)(ii) (1994). An application for a conventional wiretap shall include "a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted . . . ."

[43] *See* Goldsmith, *supra* note 7, at 410. There are multitudes of possible scenarios in which a person may try to evade detection. First, a person could avoid detection by frequently switching from his home telephone to his cellular telephone (or several cellular telephones). Another manner in which a person could thwart detection would be to go from one public pay telephone to another.

many criminals remain engaged in relevant conversations on a continuous basis while moving from one location to the next.[44] But, as criminals became more sophisticated, so did technology, allowing officers to easily target criminals who moved from one location to the next.[45]

Not surprisingly, the roving wiretap is the federal investigator's dream, because it lacks the requirements of specifying the exact location or showing probable cause to believe that the place from where the communication is to be intercepted is being used in connection with some offense.[46]

C. *Statutory Differences Between Conventional and Roving Wiretaps*

The ECPA added § 2518(11) and (12) to the conventional wiretap statute.[47] The statute, providing for roving wiretaps, differs from conventional wiretaps in four respects. First, it requires a higher level of authority to authorize an application for a roving wiretap than is required to authorize an application for a conventional wiretap.[48] Second, unlike conventional wiretap applications, which only require that the identity of the target be given *if known*, the roving wiretap application *must* provide the identity of the target.[49] Third, the roving wiretap application does not require the law enforcement officer to state the specific location of the place from where the communication is to be intercepted.[50]

---

[44] *See id.* This concern is more likely applicable to subsection (a) of § 2518(11). This subsection deals with roving "bugs." A "bug" is an instrument that can be placed in small hidden areas, such as a fire detector of a hotel room, and pick up audio or video communications that occur in the hotel room. This subsection was not amended by the 1998 amendments.

[45] *See id.* (explaining that advances in technology allowed law enforcement officials to wiretap criminals who moved from one location to the next to evade surveillance).

[46] After being granted a roving wiretap, the investigating officer has free reign to place the wiretap anywhere the target goes. *See* 1 FISHMAN & MCKENNA, *supra* note 20, at 9-14 (explaining that "[o]nce a roving intercept order is issued, there is no express limitation on the number of places in which the government can install listening devices or telephones it can tap, and the decision in each instance [is] an executive rather than a judicial one"). *But see id.* at 9-14 n.30 (explaining that often investigators are left to ensure that searches do not violate the Fourth Amendment).

[47] *See* Electronic Communications Privacy Act, § 106(d)(3), 100 Stat. 1848, 1857 (1986). The relevant provision for this Note is § 2518(11)(b) concerning "wire or electronic communication."

[48] *See* 18 U.S.C. § 2518(11)(b)(i) (1994), *amended by* Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998).

[49] *Compare* 18 U.S.C. § 2518(1)(b)(iv) (1994) (conventional wiretap) *with* 18 U.S.C. § 2518(11)(b)(ii) (1994), *amended by* Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998) (roving wiretap).

[50] In essence, this is where the statute got the name "roving." The wiretap is roving because it need not be static—it may rove from telephone to telephone. This is different from a conventional wiretap, which must include in the application "a particular description of the

Finally, to obtain a roving wiretap, there need not be a probable cause finding by a judge that the place from where the communication is being intercepted is being used in connection with some criminal offense.[51]

1. *High-Level Officials*

The first requirement in an application for a roving wiretap is that it be sought by a "high-level federal official."[52] The roving wiretap statute requires authorization for an application to be given by "the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General."[53] Though the legislative history of the 1986 Amendments makes no mention of the reasoning behind this requirement, it seems to exist to protect against potential abuse.[54] There is a greater potential for abuse because a roving wiretap enables federal officials to follow the target from one location to the next, monitoring every phone conversation the suspect makes during the day.[55] Accordingly, it is proper to require a higher level official to authorize such an application.[56]

2. *Requiring the Target's Identity*

A further attempt to guard against the inherent abuse associated with a roving wiretap is the requirement that the applicant: "identif[y] the person believed to be committing the offense and whose communications are to be intercepted . . . ."[57]

---

nature and location of the facilities from which or the place where the communication is to be intercepted." 18 U.S.C. § 2518(1)(b)(ii) (1994).

[51] This, too, is a major deviation from the standards of a conventional wiretap. A conventional wiretap application states that there must be a probable cause finding that the place from where the interception is being taken is involved in or is about to be involved in criminal activity. *See* 18 U.S.C. § 2518(3)(d) (1994).

[52] By "high-level federal official," this Note indicates that § 2518(11) requires that an application by a federal law enforcement officer be authorized by an authority higher than that required to authorize conventional wiretaps.

[53] 18 U.S.C. § 2518(11)(b)(i) (1994), *amended by* Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998); *cf.* 18 U.S.C. § 2516(1) (1994) (allowing a conventional wiretap to be ordered by any "Deputy Assistant Attorney General in the Criminal Division").

[54] *See* Fishman, *supra* note 6, at 50. This Note indicates that "a roving tap . . . is potentially far more intrusive into privacy than a standard interception order, so it is even more important to centralize the policy decisions in a 'publicly responsible official subject to the political process.'" *Id.* (quoting S. REP. NO. 90-1097, at 2185 (1968)).

[55] *See id.* at 62.

[56] *See id.* at 50 (explaining that this leaves a decision as important as one to grant a roving wiretap to a "publicly responsible official subject to the political process").

[57] 18 U.S.C. § 2518(11)(b)(ii) (1994), *amended by* Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998).

This identity requirement is narrower than that for conventional wiretaps, which require that the identity of the person be made available *only if* it is known.[58] Requiring federal investigators to identify the criminal suspect may have been Congress's effort to substitute the particularity of the target's identity for the particularity of the location or place of the wiretap.[59]

3. *Specification of Location*

The third difference between a roving wiretap and a conventional wiretap is the location requirement; this difference is the essence of "roving surveillance." Unlike conventional wiretap applications, which must state in the application the locality from where the communication is to be intercepted,[60] the location of where a roving wiretap is to be used need not be present in the application. As discussed previously, Congress purposely took away the "location" requirement in promulgating this statute[61] because Congress's purpose was to enable federal law enforcement officials to wiretap suspects who were intentionally trying to "thwart interception by changing facilities."[62]

4. *Requirement of Probable Cause of Criminal Activity in Location to Be Intercepted*

The final difference between the statutory requirements of the roving wiretap and the conventional wiretap is the requirement of a probable cause showing of

---

[58] *See* 18 U.S.C. § 2518(1)(b)(iv) (1994); *see also* 1 FISHMAN & MCKENNA, *supra* note 20, at 9-6 (explaining that the requirement that the target be identified in the application for a roving wiretap is more stringent than the requirement in a conventional wiretap application, which requires the target's identity be disclosed if it is known).

[59] *See* Fishman, *supra* note 6, at 51 (observing that this requirement is intended to limit the availability of roving wiretaps); *see also* United States v. Petti, 973 F.2d 1441, 1445 (9th Cir. 1992) (observing that the original roving wiretap statute's requirement of identifying the target helped to prevent roving wiretaps from being unconstitutionally broad). This Note argues that this requirement alone is not enough to meet the particularity requirement of the Fourth Amendment. Only when coupled with the "purpose to thwart" requirement of the original roving wiretap statute is the particularity requirement met.

[60] *See supra* note 7 and accompanying text.

[61] The purpose of the 1986 amendments to the wiretap statute was to:

> set[ ] out new rules for the specificity required in the description of the place where the interceptions of wire and oral communications are to occur. The Committee finds such a provision necessary to cover circumstances under which law enforcement officials may not know, until shortly before the communication, which telephone line will be used by the person under surveillance.

S. REP. NO. 99-541, at 31 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585.

[62] *Id.* at 32; *see also infra* notes 63–69 and accompanying text.

criminal activity at the location of the place to be intercepted. A conventional wiretap application requires that the applicant have probable cause to believe that the place from where the communications are to be intercepted is being used for criminal activity.[63] This probable cause requirement is excluded from the roving wiretap statute,[64] thereby allowing federal investigators to tap any phone from any location that a target uses regardless of whether that phone is in a public place, the suspect's home, or even in the home of an innocent third party.

The statutory differences discussed above greatly relax the requirements of a wiretap application for roving wiretaps, and yet as originally enacted, the roving wiretap statute required an applicant to carry an extra burden of proof—namely that the officer-applicant demonstrate that the suspect was purposely trying to evade interception.[65] Thus, prior to the 1998 amendment, roving wiretaps, while arguably intrusive, appeared to be constitutional because of the previously discussed statutory safeguards.

D. *Roving Made Much Easier—The 1998 Amendment*

The 1998 amendment to the roving wiretap statute replaced the "purpose to thwart" requirement in the original statute with the "could have the effect of thwarting" standard along with other changes.[66] In replacing the "purpose to thwart" requirement, Congress removed a fundamental safeguard in protecting against abuses by the issuance of roving wiretaps. This Section analyzes the way in which the amendment was brought about and the effect of the amendment on the roving wiretap statute.

1. *Amendment by Sneak Attack*

Near the close of the 105th Session of Congress "in the legislative dead of night, Congress gave law enforcement unprecedented new power to wiretap [private] communications."[67] With little warning and even less legislative

---

[63] The statute states a judge may order a wiretap if the judge determines on the basis of the application that:

> except as provided in subsection (11), there is *probable cause* for belief that the facilities from which, or the place where, the wire ... communication[ ] [is] to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

18 U.S.C. § 2518(3)(d) (1994) (emphasis added).

[64] *See* 18 U.S.C. § 2518(11) (1994 & Supp. IV 1998).

[65] *See* § 2518(11)(b)(ii) (1994).

[66] *See* 18 U.S.C. § 2518(11)(b) (1994 & Supp. IV 1998).

[67] Dan Gillmor, *Roving Wiretap Power OK'd Analysis: Congress Granted Law Enforcers More Authority to Monitor Your Electronic Communications*, BALT. SUN, Oct. 19, 1998, at 1C.

dialogue, the 105th Congress amended the roving wiretap statute and took away a key mens rea element. In its place, Congress interjected a standard that even Barney Fyffe[68] could satisfy.[69] It is unimaginable how an amendment, which loosens standards on an already arguably intrusive law, could pass without so much as a committee hearing.

The amendment to the roving wiretap statute[70] was added during the conference report for the intelligence appropriations bill[71] as opposed to the earlier House bill or Senate amendment to the appropriations bill.[72] Further, the Explanatory Statement of the managers of the conference did little to elucidate why the amendment was necessary to the roving wiretap statute.[73] In fact, the

---

The media was immediately alerted to the passage of the 1998 amendment to the roving wiretap statute and in the manner in which it was passed. In general, the consensus was not positive. One editorial went so far as to state, "[T]he president has not been so distracted by the current [Lewinsky] scandal as to forgo a raid on the Fourth Amendment." Nat Hentoff, *Raid on Rights*, WASH. POST, Jan. 2, 1999, at A19. Another editorial criticized the FBI, which sought the amendment, stating, "[t]he FBI always has been good at subterfuge and sneak attacks. Now it is using them on Congress." Blumner, *supra* note 1, at 29.

To further illustrate the stealth in the passage of this amendment, one can look to the telecommunications industry, which was taken by surprise. Specifically, the Cellular Telecommunications Industry Association (CTIA) was caught by surprise. The CTIA now has to determine when and how cellular carriers will have to implement any required technological changes required to fulfill the requirement of the amendment. *See Law Enforcement Flexes Wiretap Muscle in Intelligence Authorization*, COMM. TODAY, Oct. 12, 1998, at 6.

[68] Barney Fyffe is the dimwitted deputy on the 1960s television series *The Andy Griffith Show* (CBS 1960–68).

[69] For a discussion of the "could have" standard, see *infra* note 96 and accompanying text and Part IV.C.

[70] *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998).

[71] *See* H.R. CONF. REP. NO. 105-780, at 32 (1998), *reprinted in* 1998 U.S.C.C.A.N. 510, 518. The amendment to 18 U.S.C. § 2518(11)(b) (1994) was included in the conference report as section 604, entitled "Wire and Electronic Communications Interception Requirements." Section 604 amends 18 U.S.C. § 2518(11), (12) (1994). *See infra* Part II.C. for changes to the statute as a result of the amendment.

[72] *See* JOINT EXPLANATORY STATEMENT OF THE COMMITTEE OF CONFERENCE, H.R. CONF. REP. NO. 105-780, at 32 (1998), *reprinted in* 1998 U.S.C.C.A.N. 510, 518.

[73] The Joint Explanatory Statement states:

> Under current law, judges issue wiretap orders authorizing law enforcement officials to place a wiretap on a specific telephone number. Criminals, including terrorists and spies, know this and often try to avoid wiretaps by using pay telephones on the street at random, or by using stolen or cloned cell telephones. As law enforcement officials cannot know the numbers of these telephones in advance, they are unable to obtain a wiretap order on these numbers from a judge in time to intercept the conversation, and the criminal is able to evade interception of this communication.

purpose behind the amendment, to prevent suspects from evading a wiretap, as indicated by the Joint Explanatory Statement, was already effectuated under the original version of the roving wiretap statute.[74] However, the sponsors of the bill removed the "purpose" requirement and substituted it with the "could have" standard.

Almost as alarming as the amendment itself is the ease in which it was passed without any legislative debate on the issue. The amendment's sponsor, Representative McCollum, stated that the amendment in effect was a very minor change to the statute.[75] Representative McCollum played upon the rhetoric of terrorism to make it appear that this amendment was badly needed.[76] He argued that the amendment was necessary because the "purpose" requirement was too difficult to meet, and he even suggested that the amendment would make the wiretap law narrower.[77] Representative McCollum's next contention was that this

---

> This provision addresses this problem by authorizing judges to issue an order authorizing the interception of all communications made by a particular person, regardless of what telephone he may use. The provision does not change the existing law that requires law enforcement officials to show that there is probable cause to believe that the suspect has committed, or may commit, a crime. With this amendment, law enforcement officials will be required to show that there is probable cause to believe that the actions of the suspect *could have the effect of thwarting a wiretap on a specific telephone were the court to order the more typical method of wiretap, which targets a specific telephone number.*

Id. at 32, *reprinted in* 1998 U.S.C.C.A.N. 518–19 (emphasis added). Emphasis was added to the Explanatory Statement to indicate the major change to 18 U.S.C. § 2518(11)(b) (1994) as a result of the amendment.

[74] The Joint Explanatory Statement does not indicate how the original version of 18 U.S.C. § 2518(11)(b) (1994) failed to meet the purpose as put forth by the Conference managers. In fact, § 2518(11)(b) was originally enacted to combat the very thing that the Conference Report addresses—a suspect who tries to evade detection. There is no indication that this effort was being retarded by the requirement of a showing of a purpose to evade surveillance as required by the roving wiretap statute.

[75] *See* 144 CONG. REC. H9725, H9731 (daily ed. Oct. 7, 1998) (statement of Rep. McCollum). Representative McCollum noted that the amendment had "given pause to some . . . Members" of the Conference report. *Id.* He tried to dismiss this concern by arguing that the amendment was a small change to the statute but was a "very significant change in the law dealing with wiretaps." *Id.*

[76] *See id.* A similar argument was made for expanded wiretap surveillance after the 1995 bombing of the Alfred P. Murrah federal building in Oklahoma City. *See* Kopel & Olson, *supra* note 9, at 312–13. Kopel and Olson observe that during the debate of the Antiterrorism and Effective Death Penalty Act of 1996, many called for expanded wiretap surveillance because they thought that current law restricted the use of wiretaps for investigating suspected terrorism. However, they point out that out of 2130 wiretap applications in 1993–94, not a single one was for terrorism. *See id.*

[77] *See* 144 CONG. REC. H9725, H9731 (daily ed. Oct. 7, 1998) (statement of Rep. McCollum). Representative McCollum made several comments that deserve attention. First, he stated that this particular issue had been the subject of much debate. *See id.* To date, no debate concerning this amendment has been found other than the brief statements made by

amendment was necessary because the intent requirement was very difficult to prove.[78] It is true that the intent to evade standard may be difficult to establish, but it is this "purpose" requirement that helps to substitute for the particularity requirement of the Fourth Amendment and which has been relied upon by courts to uphold the constitutionality of the amendment.

Representative Barr, ironically a former federal prosecutor and CIA analyst, rose in opposition not only to the amendment but also to the manner in which it was being introduced.[79] He argued that this amendment was not a minor change to the existing law but was "a fundamental shift in wiretapping procedures in this country."[80] Barr stated that without the "purpose" requirement, the roving wiretap statute would raise serious civil liberties and privacy rights issues.[81]

In response to Representative Barr's arguments, Representative McCollum again argued that the amendment was a minor change and resumed to arguing that it is a "terrorism issue."[82] He further stated that the amendment only allows the issuance of a roving wiretap if a judge finds that the target's "actions show he

---

Representative McCollum and an effort by Representative Barr to have this issue taken out of Conference and put into committee. Representative McCollum may have been making reference to the fact that a similar provision was offered as a part of the 1996 Antiterrorism Act; however, that provision was soundly defeated.

The final statement put forth by Representative McCollum in support of the amendment is that this amendment would make the wiretap law narrower. *See id.* This statement is without merit. Representative McCollum stated that under the amendment, once the target walks away from a pay phone where a roving wiretap was placed, the phone cannot be tapped anymore. *See id.* This is true with the original version of 18 U.S.C. § 2518(11)(b) (1994). Representative McCollum concludes his selling of the bill by stating that no "[m]ember should mistake this as some major addition to the wiretap laws." *Id.*

[78] *See id.*

[79] *See id.* at H9737.

[80] *Id.*

[81] *See id.* Representative Barr argued that with this amendment a roving wiretap could be ordered without the showing of a purpose on the part of the target to thwart conventional electronic surveillance means. *See id.* He also pointed out that this amendment is not limited to "foreign intelligence surveillance" but to any case in which federal officials seek a roving wiretap—be it for domestic crimes such as money laundering or international crimes such as terrorism. *See id.* This observation seems to indicate that many in Conference Committee were persuaded by Representative McCollum's remarks that this amendment was necessary to combat terrorism. However, as pointed out by Representative Barr, nowhere in the statutory language or legislative history is it indicated that Congress's intent was for this law to apply only to terrorism situations. *See id.*

[82] *Id.* This Note uses the term "terrorism issue" to indicate Representative McCollum's insistence on trying to indicate that this amendment was limited to terrorists. Though Representative McCollum never states verbatim that the bill was limited to terrorists, it appears that he was trying to push the issue to gain empathy from his fellow Representatives. For example, in defending the amendment, Representative McCollum stated that the amendment "permits the court-ordered wiretap that follows the *criminal terrorist suspect* to whatever phone he uses . . . ." *Id.* (emphasis added).

is trying to evade the tap . . . ."[83] However, with the amendment's elimination of the "purpose" requirement, this is simply not true. The amendment to the statute allows a roving wiretap to be issued if the suspect's "actions could have the effect of" evading the tap.[84] The "could have" standard is much easier to meet than the "purpose to thwart" standard.[85]

Representative Barr attempted to remove section 604 from the appropriations bill so that it could be fully debated at a later time.[86] However, in an effort to pass the intelligence appropriations bill without delay, his proposal was soundly defeated.[87] Both the House and the Senate adopted the Conference Committee version, and President Clinton signed it into law on October 20, 1998.[88]

The courts that have decided cases involving the original roving wiretap statute[89] declared it to be constitutional.[90] In each of these cases, the individual courts relied heavily upon the "purpose . . . to thwart interception"[91] requirement.[92] Thus, it follows that the amended statute is unconstitutional because it deletes a major element that was used by the courts in finding the statute constitutional.[93] Without the "purpose to thwart" requirement, the statute fails to meet the Fourth Amendment's particularity requirement.[94]

---

[83] *Id.*

[84] The amended version of the statute reads in pertinent part: "the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility . . . ." Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998).

[85] *See infra* Part IV.C.

[86] *See* 144 CONG. REC. H9725, H9739 (daily ed. Oct. 7, 1998) (statement of Rep. Barr).

[87] The vote was 148 yeas, 267 nays, and 19 not voting. *See id.* at H9739–40.

[88] *See* Statement on Signing the Intelligence Authorization Act for Fiscal Year 1999, 34 WEEKLY COMP. PRES. DOC. 2082 (Oct. 20, 1998).

[89] 18 U.S.C. § 2518(11)(b) (1994).

[90] For a discussion on decisions of courts upholding the constitutionality of the original roving wiretap statute, see *infra* Part III.C.

[91] 18 U.S.C. § 2518(11)(b)(ii) (1994).

[92] For a discussion on the reasoning of courts which found the original roving wiretap statute constitutional, see *infra* Part III.C.

[93] *See id.*

[94] The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized.*

U.S. CONST. amend. IV (emphasis added).

2. *Replacement of the "Purpose to Thwart" Requirement*

As a result of the 1998 amendments, the requirement that an applicant for a roving wiretap had to make "a showing of a purpose, on the part of [the target], to thwart interception"[95] was replaced by the "could have" standard. The "could have" standard appears in the amendment to the roving wiretap statute, which reads in pertinent part: "[T]he applicant makes a showing that there is probable cause to believe that the person's actions *could have the effect of thwarting interception* from a specified facility . . . ." [96] The addition of subsection (b)(iv) is the other change to § 2518(11)(b) as a result of the amendment. Subsection (b)(iv) states: "the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was *reasonably proximate* to the instrument through which such communication will be or was transmitted."[97]

According to the Joint Explanatory Statement, this subsection was added to "ensure that only the conversation of the suspect (and with whomever he speaks) is intercepted . . . ."[98] The Joint Explanatory Statement further stated that the requirements of this subsection may only be met when it is reasonable to assume the suspect is "reasonably proximate" to the particular phone being tapped.

The "reasonably proximate" standard also loosens the limitations placed upon roving surveillance in the original roving wiretap statute. No longer are officials required to wait until the target is on the telephone or evidences an intent to use the telephone, but officials can now begin to intercept a communication when the target is "reasonably proximate" to the telephone.[99] This ability to wiretap a telephone to which a suspect is "reasonably proximate" will allow the government to intercept more innocent conversations than a conventional wiretap would permit.[100]

III. ENSURING ROVING DOES NOT GO TOO FAR— "THE PURPOSE" REQUIREMENT

The "purpose to thwart" requirement in the original roving wiretap statute guarded against wide open invasion of privacy occurrences.[101] This Part

---

[95] 18 U.S.C. § 2518(11)(b)(ii) (1994), *amended by* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 604, 112 Stat. 2396, 2413 (1998).

[96] 18 U.S.C. § 2518(11)(b) (1994 & Supp. IV 1998) (emphasis added).

[97] *Id.* (emphasis added).

[98] JOINT EXPLANATORY STATEMENT OF THE COMMITTEE OF CONFERENCE, H.R. CONF. REP. NO. 105-780, at 33 (1998), *reprinted in* 1998 U.S.C.C.A.N. 510, 519.

[99] *See* 18 U.S.C. § 2518(11)(b) (1994 & Supp. IV 1998).

[100] *See infra* Part IV.D.

[101] The amended version of § 2518(11)(b)(ii), which does not contain the "purpose . . . to thwart" language, will have a significant impact on personal privacy as it will now be much

describes the importance of the "purpose" requirement in statutory context and the reliance placed upon it by courts in finding the original roving wiretap statute constitutional.

A. *Purpose—King of the Mens Rea Mountain*

In order to obtain a roving wiretap under the original roving wiretap statute, the applicant had to make "a showing of purpose, on the part of [the suspect], to thwart interception...."[102] In determining the meaning of a statute, it is imperative to begin with the statutory language.[103] Accordingly, when trying to ascertain the requirements to obtain a roving wiretap statute, one must look to the statute. The requirement in the ECPA, which provided the most protection against the arbitrary issuance of a roving wiretap and which was relied upon by the courts[104] in upholding the constitutionality of the statute, was the "purpose to thwart" requirement.

"Purpose" is atop the list of the *Model Penal Code*'s culpability requirements[105] and thus is the highest scienter requirement recognized by the American Law Institute's *Model Penal Code*. According to the drafters of the *Model Penal Code*, an action is not purposeful "unless it was [the actor's] conscious object to perform an action of that nature or to cause such a result."[106]

Although a person does not commit a statutory offense by trying to evade a wiretap, Congress intended the mens rea element to be present prior to a valid issuance of a roving wiretap. The legislative history is not conclusive as to why Congress used the term "purpose."[107] However, examples given by the drafters of the ECPA illustrate that they intended a requirement similar to the definition used by the *Model Penal Code*.[108] In addition, as roving wiretaps are more intrusive

---

easier for federal law enforcement officials to conduct roving wiretaps.

[102] 18 U.S.C. § 2518(11)(b)(ii) (1994).

[103] Justice Frankfurter instructed his students that the most fundamental step in statutory interpretation is to "(1) [r]ead the statute; (2) read the statute; (3) read the statue!" HENRY J. FRIENDLY, BENCHMARKS 202 (1967).

[104] *See infra* Part III.C.

[105] *See* MODEL PENAL CODE § 2.02(2)(a) (1985). The Code reads in pertinent part:

> A person acts purposely with respect to a material element of an offense when:
>
> (i) if the element involves the nature of his conduct or a result thereof, it is his conscious object to engage in conduct of that nature or to cause such a result; and
>
> (ii) if the element involves the attendant circumstances, he is aware of the existence of such circumstances or he believes or hopes that they exist.

Id. But see generally Sharon L. Davies, *The Jurisprudence of Willfulness: An Evolving Theory of Excusable Ignorance*, 48 DUKE L.J. 341 (1998) (explaining that the mens rea term "willful" may be the highest scienter requirement).

[106] MODEL PENAL CODE § 2.02 commentary at 233 (1985).

[107] *See* Fishman, *supra* note 6, at 54–56.

[108] For example, a person who tells others that he is switching phones to avoid detection is

than conventional wiretaps,[109] Congress required a showing of need in order to obtain a roving wiretap.[110]

B. *What Evidences a "Purpose to Thwart"?*

The requirement of a probable cause showing of "purpose to thwart" is subject to varied interpretation as to what exactly illustrates a purpose to thwart by a suspect.[111] Fortunately, Congress gave examples of what it envisioned in the Senate report, which described "an alleged terrorist who went from phone booth to phone booth numerous times to avoid interception."[112] A further example given in the Report is: "A person whose telephone calls were intercepted who said that he or she was planning on moving from phone to phone or to pay phones to avoid detection also would have demonstrated that purpose."[113] However, such purposeful action on the part of the suspect is no longer a prerequisite to the roving wiretap.[114]

---

one example of a "purpose to thwart interception" included in the legislative history of the original roving wiretap statute. *See* S. REP. NO. 99-541, at 32 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3586. This example is analogous to the definition of "purpose" as put forth by the *Model Penal Code*—a conscious objective to cause such a result (here avoiding surveillance).

[109] *See supra* note 11.

[110] *See* Fishman, *supra* note 6, at 52 (explaining that an applicant must show why a roving wiretap is needed). There is some speculation that the "purpose" requirement may not have been solely for the protection of privacy interests but also for an interest in easing the burden of the nation's telephone companies. *See id.* at 55–56 (explaining that one reason for the "purpose" requirement was over concern raised by lobbyists for the telephone companies who were fearful that roving wiretaps may be too burdensome because they would not be given adequate notice).

[111] In determining if a suspect was "purposely" seeking to evade a conventional wiretap, courts are left in a precarious position. They must rely on the affidavits of the investigating officer to illustrate the evasive techniques employed by the suspect. The judge must determine if the "techniques" employed by the suspect are evidence of a purpose to evade the wiretap. The difficulty in such a determination is that the target is not available to explain why he switched telephones. A suspect does not have the opportunity to explain his actions until after he has been charged—and is now a defendant. *See* United States v. Villegas, No. 92 CR. 699 (CSH), 1993 WL 535013, at *10, *11 (S.D.N.Y. Dec. 22, 1993) (illustrating an example in which the defendant argued, unsuccessfully, that his actions did not evidence a "purpose" to thwart detection).

[112] S. REP. NO. 99-541, at 32 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3586.

[113] *Id.*

[114] With the "purpose" requirement removed, this leaves courts in a precarious position. Courts will now have to define what type of conduct is required to be shown in order to obtain a roving wiretap. The legislative history of the 1998 amendment is totally void of any indication of what type of conduct would illustrate compliance with the "could have" standard of the new statute. This Note sets forth one example in which a court could reasonably believe that the new "could have the effect of" standard would be met. *See infra* Part IV.C. This example is

C. *Case History of the Roving Wiretap—Reliance on the "Purpose" Requirement*

The case authority on roving wiretaps is not voluminous by any means.[115] Thus far, only two federal circuits have decided on the constitutionality of the roving wiretap statute.[116] Unfortunately, *United States v. Petti*[117] is the only federal circuit court case that contains more than a one-paragraph analysis of the constitutionality of the roving wiretap statute.[118]

1. United States v. Petti

In *United States v. Petti*,[119] Petti appealed the decision of the district court that denied his motion to suppress the wiretap surveillance on grounds that the roving wiretap statute was unconstitutional.[120] Specifically, the defendant argued that the absence of the location from where the communication was to be intercepted in an application for a wiretap violated the particularity requirement of the Fourth Amendment.[121] Put differently, the defendant argued that the roving wiretap statute was unconstitutional because it did not require that the location of the place from which the communication was to be intercepted be known at the

---

indicative of the types of conduct that courts will face when deciding whether to issue a roving wiretap under the new standard.

[115] A Westlaw electronic search indicated that six cases addressed the topic of roving wiretaps as of March 3, 2000. Search of WESTLAW, Allfeds database (Mar. 3, 2000). More case authority may address "roving bugs," which appear in 18 U.S.C. § 2518(11)(a) (1994). As the subsection concerning roving bugs does not have the "purpose" requirement that is contained in the roving wiretap statute, this Note will limit analysis of cases to those concerning roving wiretaps.

[116] *See, e.g.*, United States v. Gaytan, 74 F.3d 545 (5th Cir. 1996); United States v. Petti, 973 F.2d 1441 (9th Cir. 1992).

[117] 973 F.2d 1441 (9th Cir. 1992).

[118] The only other circuit addressing the constitutionality of the roving wiretap statute deferred to the reasoning of the Ninth Circuit in *Petti*. *See* United States v. Gaytan, 74 F.3d 545, 553 (5th Cir. 1996) (upholding the § 2518(11)(b) without analysis, instead "join[ing] the Ninth Circuit['s]" analysis). Several district courts have also fielded the question of the constitutionality of § 2518(11)(b). *See, e.g.*, United States v. Silberman, 732 F. Supp. 1057 (S.D. Cal. 1990); United States v. Parks, No. 95 CR. 510, 1997 WL 136761 (N.D. Ill. Mar. 24, 1997); United States v. Villegas, No. 92 CR. 699 (CSH), 1993 WL 535013 (S.D.N.Y. Dec. 22, 1993); *see also* United States v. Bianco, 998 F.2d 1112, 1120–24 (2d Cir. 1993) (analyzing the constitutionality of the "roving bug" statute—18 U.S.C. § 2518(11)(a) (1994)).

[119] 973 F.2d 1441 (9th Cir. 1992).

[120] *See id.* at 1443.

[121] *See id.* at 1444. The Fourth Amendment requires that "no Warrants shall issue, but upon probable cause, ... and *particularly describing the place to be searched*...." U.S. CONST. amend. IV (emphasis added).

time the wiretap order is issued.[122]

On appeal, the circuit court upheld the district court's decision; however, it provided only cursory analysis.[123] The court based its decision on the fact that the particularity requirement could be met even if the exact location or phone to be searched is not specified.[124] Reasoning that it might be impossible for federal agents to know in advance from what location a defendant would use the telephone, the court stated that agents could provide other information that would effectuate the purpose of the particularity requirement.[125]

In *Petti*, the particularity requirement was met because the target was identified in the application, and the government was able to "establish[ ] to the court's satisfaction that it [was] impossible to specify the facilities because it [was] the suspect's *purpose to thwart interception* by changing them."[126] Thus, the "other information" that effectuated the particularity requirement was the defendant's purpose to evade the wiretap.[127] Moreover, the court also declared that the target of the interception must be identified under the statute, and this ensures that the particularity requirement will be met.[128]

2. *In Accord with* Petti

Of the federal courts that have addressed the constitutionality of the original roving wiretap statute, all have found it to be constitutional.[129] In each of these cases, the courts, in upholding the roving wiretap statute, relied on the statute's requirement of showing a purpose to thwart surveillance by the target.[130]

---

122 *See Petti*, 973 F.2d at 1444.

123 *See id.* at 1445 (holding that the district court did not err when it found § 2518(11)(b) to be constitutional).

124 *See id.* at 1444 (citing United States v. Karo, 468 U.S. 705, 718 (1984) (holding that law enforcement officers may satisfy the particularity requirement by providing information other than the exact location)).

125 *See id.* The purpose of the particularity requirement is to prevent general searches. *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (explaining that "the manifest purpose of [the] particularity requirement was to prevent general searches"); *see also infra* notes 135–44 and accompanying text.

126 *See Petti*, 973 F.2d at 1445 (emphasis added).

127 *See id.* The court explained that "the statute excuses failure to identify the particular telephone facilities to be surveilled only if the government establishes to the court's satisfaction that it is impossible to specify the facilities because it is the suspect's purpose to thwart interception by changing them." *Id.*

128 *See id.*

129 *See, e.g.*, United States v. Gaytan, 74 F.3d 545, 553 (5th Cir. 1996); United States v. Silberman, 732 F. Supp. 1057, 1063 (S.D. Cal. 1990); United States v. Parks, No. 95 CR. 510, 1997 WL 136761, at *18 (N.D. Ill. Mar. 24, 1997).

130 *See* 18 U.S.C. § 2518(11)(b)(ii) (1994 & Supp. IV 1998).

The analysis of the constitutionality of the original roving wiretap statute that provides the most exhaustive analysis is provided by the district court in *United States v. Silberman.*[131] The *Silberman* court looked to legislative history to infer what Congress's intent was in regard to the particularity requirement of the Fourth Amendment and how that intent was to be met with the roving wiretap statute. The court recognized that "Congress envisioned a 'relaxed specificity order' in response to situations [in which the target was purposefully evading detection]."[132] It found that the relaxed particularity requirement of the statute complied with the Fourth Amendment because the "purpose" requirement and the other requirements enumerated in the statute rescued it from being overly broad.[133] The reliance on the "purpose" requirement along with the other requirements seems to indicate that, taken together, the statute is constitutional. Thus, when one of the factors is taken away, the constitutionality of the statute is threatened.[134]

IV. THE ABSENCE OF THE "PURPOSE TO THWART" REQUIREMENT RENDERS THE ROVING WIRETAP STATUTE UNCONSTITUTIONAL

> *Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.*[135]

Electronic interception of communications is inherently intrusive and must be narrowly tailored to conform to constitutional standards. Namely, warrants for electronic interception must meet the same standards as those imposed on conventional search warrants. This means that warrants for electronic surveillance of communications must meet the requirements set forth in the Fourth

---

[131] 732 F. Supp. 1057 (S.D. Cal. 1990), *aff'd* 973 F.2d 1441 (9th Cir. 1992). The Ninth Circuit deferred to the discussion in this case in its decision upholding the district court's decision that 18 U.S.C. § 2518(11)(b) (1994 & Supp. IV 1998) was constitutional. *See* United States v. Petti, 973 F.2d 1441, 1445 n.4 (9th Cir. 1992), *aff'g* 732 F. Supp. 1057 (S.D. Cal. 1990); *see also supra* Part III.C.1.

[132] *Silberman*, 732 F. Supp. at 1062 (quoting S. REP. NO. 99-541, at 31 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585).

[133] *See Silberman*, 732 F. Supp. at 1062–63. The court found two other requirements of the statute to be dispositive in its decision. First, the statute limits the number of people who may issue a roving wiretap. Second, the statute limits interception of the conversations to only those of the target. *See id.*

[134] The courts, which addressed the constitutionality of the original roving wiretap statute, did not plainly state that the "purpose" requirement was more important than any of the other requirements. However, roving wiretaps evolved out of the frustration encountered by federal investigators when a suspect was evading the detection of a conventional wiretap. It is therefore unremarkable to suggest that the "purpose" requirement of the original roving wiretap statute is the most important factor upon which the courts relied.

[135] Berger v. New York, 388 U.S. 41, 63 (1967) (Clark, J.).

Amendment, which provides:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized.*[136]

Both Title III and the ECPA put significant burdens on government officials who wished to conduct wiretap surveillance. The 1998 amendment removed the key requirement imposed by the ECPA for a roving wiretap application. By removing the "purpose" requirement from the statute, the 1998 amended roving wiretap statute is unconstitutional because it fails to meet the particularity requirement of the Fourth Amendment.

A. *The Fourth Amendment's Particularity Requirement*

The Fourth Amendment requires that a search warrant will not be issued unless it "particularly describ[es] the place to be searched . . . ."[137] By requiring specificity of the location to be searched, the Framers of the Constitution intended to prevent arbitrary searches that subject any area of a person's private dwelling to government inspection.[138] According to one scholar on the law of search and seizure, the particularity requirement protects individuals "from arbitrary and oppressive searches and seizures and 'roving commissions.'"[139]

The particularity requirement is not easily met in warrants for roving wiretaps or other electronic surveillance devices such as electronic beepers.[140] However, the Fourth Amendment has been interpreted to conform to the changing times and

---

[136] U.S. CONST. amend. IV (emphasis added).

[137] *Id.*

[138] *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (explaining that "the manifest purpose of [the] particularity requirement was to prevent general searches"); *see also* United States v. Karo, 468 U.S. 705, 718 (1984) (requiring that the particularity requirement be met in a warrant for an electronic beeper); Andresen v. Maryland, 427 U.S. 463, 480 (1976) (observing that the Framers of the Constitution included the particularity requirement to ensure that a search warrant is not too broad); 2 JOHN WESLEY HALL, JR., SEARCH AND SEIZURE § 43:10, at 621 (2d ed., 1993) (finding that the particularity requirement is an imperative requirement of any warrant); Russell W. Galloway, Jr., *Basic Fourth Amendment Analysis*, 32 SANTA CLARA L. REV. 737, 768 (1992) (noting that the particularity requirement "is crucial for preventing general searches and seizures").

[139] 2 HALL, *supra* note 138, § 43:11, at 621.

[140] This Note means "particularity requirement" in its traditional sense—the location of the person or place to be searched. Roving wiretaps and search warrants for electronic beepers cannot specify location because it is impossible to forecast where the target will use a telephone or where an electronic beeper may travel.

has "kept up" with technological advancements.[141] The Supreme Court has recognized that the use of electronic devices sometimes makes it more difficult to meet the particularity requirement of the Fourth Amendment.[142] For example, the Supreme Court in *United States v. Karo* held that although the exact location of the place to be searched could not be identified, a search warrant was still required.[143] The Court further held that though the exact location could not be identified, the government could meet the particularity requirement by providing other information.[144]

B. *Failing to Meet the Standard*

The amended version of the roving wiretap statute[145] is unconstitutional because it fails to meet the particularity requirement of the Fourth Amendment. Although the exact location of the place to be searched where a telephone will be tapped does not have to be known,[146] there must be other information provided in the warrant application that sufficiently defines the place to be searched in order to meet the particularity requirement.[147] This "other information" standard was met in the original roving wiretap statute with the requirement of a showing of

---

[141] The Fourth Amendment is not to be read literally. *See* Sean R. O'Brien, Note, United States v. Leon *and the Freezing of the Fourth Amendment*, 68 N.Y.U. L. REV. 1305, 1308–09 (1993) (explaining that because technology available to law enforcement allows greater intrusions into individuals' lives, any changes should be translated into Fourth Amendment law).

[142] *See Karo*, 468 U.S. at 718.

[143] *See id.*

[144] It was impossible for the government to identify the place to be searched because the purpose of the electronic beeper was to aid the agents in determining the location of illegal activity. *See id.* at 715–17. The government argued that because it was impossible to meet the particularity requirement, no search warrant should be required. *See id.* at 718. The Court disagreed but held that the particularity requirement could be met by providing the following information: a description of the object into which the beeper would be placed, the circumstances that led the agents to wish to install the beeper, and the length of time for which the beeper surveillance was requested. *See id.* According to the Court, these other factors would satisfy the particularity requirement. *See id.*

[145] *See* 18 U.S.C. § 2518(11)(b) (1994 & Supp. IV 1998).

[146] *See, e.g.*, *Karo*, 468 U.S. at 718; United States v. Gaytan, 74 F.3d 545, 553 (5th Cir. 1996); United States v. Petti, 973 F.2d 1441, 1445 (9th Cir. 1992); United States v. Silberman, 732 F. Supp. 1057, 1063 (S.D. Cal. 1990); United States v. Parks, No. 95 CR. 510, 1997 WL 136761, at *18 (N.D. Ill. Mar. 24, 1997); *see also* WAYNE R. LAFAVE & JEROLD H. ISRAEL, CRIMINAL PROCEDURE § 3.4(3), at 159 (2d ed. 1992) (explaining that the particularity requirement of the Fourth Amendment can be met in the absence of "[a]bsolute perfection in description" if enough of a description is given to allow an officer to reasonably ascertain the place to be searched).

[147] *See Karo*, 468 U.S. at 718 (holding that other information provided by law enforcement agents may meet the particularity requirement).

"purpose" to evade interception.[148] The amended statute does not have the "purpose" requirement and is, therefore, unconstitutional.

As discussed previously, the "other information" consisted of the following: showing that the target was purposely trying to evade interception; demonstrating the identity of the target; and specifying that only high-ranking federal officials could order a roving wiretap.[149] The courts that upheld the constitutionality of the roving wiretap statute all relied on these factors to find that the statute met the particularity requirement.[150]

C. *The "Could Have the Effect of Thwarting" Standard Will Result in General Searches*

The 1998 amendment's "could have" standard renders the statute unconstitutional because it is a standard which is so easily met that it will enable federal law enforcement officials to conduct general searches.[151] Without having to show that a suspect is purposely trying to evade detection, a law enforcement officer will be able to obtain a roving wiretap based on everyday occurrences. In essence, the "could have" standard will give officers "a roving commission to 'seize' any and all conversations."[152]

Proponents of the amended roving wiretap statute might argue that the requirement of identifying the target will prevent general searches. However, the Supreme Court rejected a similar argument in *Berger v. New York*.[153] In *Berger*, the Court recognized that the statute at issue required the identity of the person whose communications were to be recorded.[154] The Court held that this requirement did not save the statute and "[did] no more than identify the person whose constitutionally protected area is to be invaded rather than 'particularly

---

[148] Congress envisioned a "relaxed specificity order" in the original roving wiretap statute. United States v. Silberman, 732 F. Supp. 1057, 1062 (1990). The *Silberman* court recognized that this relaxation of specificity could only comport with the Fourth Amendment if there were "sufficien[t] . . . justifications and limitations set forth in the statute." *Id.* In finding the original roving wiretap statute constitutional, the court relied heavily on the "purpose to thwart" requirement, stating that "[o]nce a judge has made a determination that the location of the search is being *purposefully* changed in order to evade detection or interception by law enforcement agents, an order with an expanded scope is clearly justified to counteract such attempted evasion." *Id.* (emphasis added).

[149] *See* 18 U.S.C. § 2518(11)(b) (1994).

[150] *See supra* Part III.C.

[151] *See* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (explaining that the purpose of the particularity requirement was to prevent general searches).

[152] Berger v. New York, 388 U.S. 41, 59 (1967).

[153] *See id.*

[154] *See id.*

describing' the communications, conversations, or discussions to be seized."[155] According to the Court, this left too much discretion to the officer executing the wiretap and was, therefore, analogous to a general search.[156]

Likewise, the "could have" standard does not prevent general searches. It is a standard that is too easily met to properly limit the intrusive nature of electronic surveillance. Officials no longer have to show that a person is intentionally going from one location to the next in an effort to evade wiretap surveillance. Rather, officers must show only that the target is going from one location to the next. For instance, an officer could merely show that by using the telephone in one's own home and then in a friend's home, a suspect "could have the effect of thwarting interception from a specified facility."[157] This results in general searches because officers will be able to conduct wiretap surveillance at any home or location in which the target makes a call without having to show that the target went to the different location to evade a conventional wiretap.

Under the amended roving wiretap statute, a judge must issue a roving wiretap if the applicant can make a probable cause showing that the suspect's "actions could have the effect of thwarting interception from a specified facility."[158] Accordingly, a judge would have to issue a roving wiretap in the following scenario: Federal investigators are investigating a "small town" doctor for RICO violations. The investigators have already obtained a search warrant to wiretap the doctor's home telephone but are frustrated because the doctor is frequently out of his home making "house calls." Under the amended roving wiretap statute, the investigators can get a roving wiretap because the doctor's actions (making house calls) *could have* the effect of thwarting a conventional wiretap. Under the original version of section 2518(11), the investigators would have to show that the doctor was going on these "house calls" with the purpose of thwarting the conventional wiretap. However, under the amended version, the investigators now only have to make a showing that by going from home to home, the doctor's actions "could have" the effect of thwarting surveillance.

The scenario described above would allow investigators to conduct a general search in violation of the Fourth Amendment. A roving wiretap issued on the

---

[155] *Id.*

[156] *See id.*

[157] 18 U.S.C. § 2518(11)(b) (1994 & Supp. IV 1998). It may seem implausible that a roving wiretap could be issued just because a suspect used a telephone at a friend's home. If, however, the suspect frequently used the telephone at his friend's home, then a roving wiretap could be issued. Under the original roving wiretap statute, such a scenario would not allow the issuance of a roving wiretap. However, under the amended version's "could have" standard, a roving wiretap would have to be issued under this same scenario. The statute requires only that the target's actions "could have the effect of thwarting interception from a specified facility." Therefore, by using a telephone other than the one on which a wiretap is placed, the suspect's actions "could have the effect of thwarting interception" and thus a roving wiretap could be issued.

[158] 18 U.S.C. § 2518(11)(b) (1994 & Supp. IV 1998).

facts in the scenario would lead to a general search because the officers would not be required to particularly describe the communications to be seized. Instead, the officers would be allowed to wiretap any phone that the doctor uses without showing that he was using the phone in an effort to conduct illegal activity or to thwart a conventional wiretap.

D. *Obtaining Wiretaps—Now Easier Than Ever*

Wiretaps are not difficult to obtain and requests for wiretaps are rarely, if ever, revoked.[159] The 1998 amendment will result in the issuance of even more roving wiretaps. Proponents of the 1998 amendment may argue that this should not be a concern because there were only twelve roving wiretaps applied for in 1997;[160] however, just the opposite is true.

So few roving wiretaps were applied for because of the difficulty in obtaining a roving wiretap under the original roving wiretap statute's "purpose" requirement.[161] The requirement of showing a "purpose to thwart" on the part of the suspect should not be seen as a difficulty but as a justified limitation on the inherent intrusive nature of roving wiretaps.[162] With the removal of the "purpose" requirement, roving wiretaps will parallel the demographics of conventional wiretaps—which is not desirable.

In the last 10 years, there have been 10,347 electronic intercept applications requested; of these, only 3 have been denied.[163] It is this type of deference to granting wiretaps that is alarming. Because wiretapping is inherently intrusive, there must be limitations on its availability.[164] It does not appear that the proscriptions on electronic surveillance result in the rejection of electronic

---

[159] For an analysis of the number of wiretaps requested and the number authorized, see generally STATISTICAL DIV., ADMIN. OFFICE OF THE UNITED STATES COURTS, 1997 WIRETAP REPORT (1998) [hereinafter 1997 WIRETAP REPORT].

[160] In 1997, there were four total applications and four authorizations for federal roving wiretaps. One was authorized in the District of Massachusetts for an investigation into an extortion operation, and three more were authorized for narcotics investigations located in New York and Virginia. In addition to the four federal roving wiretaps issued, eight were issued under state roving wiretap statutes. Seven were for investigations into narcotics, and one was issued for an investigation into gambling. *See id.* at 8, 14.

[161] Indeed, it was this "difficulty" that encouraged supporters of the amendment to seek the removal of the "purpose" requirement. *See supra* notes 77–78 and accompanying text.

[162] *See supra* notes 11, 14, and accompanying text.

[163] *See* 1997 WIRETAP REPORT, *supra* note 159, at 30. The *1997 Wiretap Report* does not break up this statistic into the different types of electronic surveillance. However, the report indicates that normally telephone wiretaps vastly outnumber the other types of electronic surveillance. For example, in 1997 telephone wiretap authorizations numbered 756, while all other types ("bugs," electronic surveillance, and a combination of types) aggregated 338. *See id.* at 27.

[164] *See supra* note 11.

surveillance applications.

Again, many proponents of electronic surveillance may argue that these statistics illustrate that law enforcement officials have sought electronic surveillance only when necessary and have followed the statutory proscriptions, which would explain the high authorization rate. However, wiretapping is not as successful as the authorization rates would lead one to believe.[165] For example, in 1997, of the 2508 interceptions of communications by the federal government, 394 resulted in incriminating intercepts—only 16%.[166] This means that the federal government intercepted 2114 communications that were completely innocent. This is where the concern lies. In one year, the federal government listened to over 2000 innocent conversations.

Of the over 2000 innocent communications that were electronically intercepted, a majority of them required a probable cause showing that the location where the interception occurred was involved in criminal activity.[167] Because roving wiretaps do not require this probable cause showing with respect to the location, it is not difficult to imagine that they intercept many nonnefarious communications. While this may seem "acceptable" in a year in which only twelve total roving wiretaps were issued, it would not be acceptable if there were one hundred roving wiretaps issued.

By removing the "purpose" requirement and replacing it with the "could have" standard, Congress has laid the foundation for increased issuance of roving wiretaps. Federal investigators will be able to utilize the roving wiretaps in situations they never would have dreamed of under the original roving wiretap statute.[168] With increased numbers of roving wiretaps being issued, there will be an increase in the number of innocent conversations that will be intercepted.[169]

---

[165] *See* HERMAN SCHWARTZ, TAPS, BUGS, AND FOOLING THE PEOPLE 26 (1977) (acknowledging twenty years ago that wiretapping had not "accomplished . . . much").

[166] *See* 1997 WIRETAP REPORT, *supra* note 159, at 21. This figure is the result of 563 interception orders that intercepted 2508 communications.

[167] This is because only a "roving" wiretap or bug allows issuance without specificity of location in the application. The *1997 Wiretap Report* does not provide how many of these intercepted "innocent" conversations were the result of roving surveillance. Because only twelve total (federal and state) roving wiretap orders were issued in 1997, it seems likely that a majority of these electronically intercepted, innocent conversations were intercepted through conventional electronic surveillance methods.

[168] *See supra* Part IV.C.

[169] Proponents of the amended roving wiretap statute may respond to this argument by arguing that minimization principles will prevent the potential for innocent conversations being intercepted. "Minimization" refers to the limits placed on what agents may and may not listen. The principle is taken from 18 U.S.C. § 2518(5), which provides, in pertinent part, that each intercept "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception" under the order. There are different ways in which minimization can be effectuated. The method most commonly utilized is to rely on the agent's good faith ability to record and listen to only conversations involving the target. *See* 1 FISHMAN

Because roving wiretaps allow interception of communications from any phone proximate to the target,[170] there is a greater probability of innocent interception than with conventional wiretaps.

The "purpose" requirement was instrumental in limiting the number of roving wiretaps that were issued.[171] If the 1998 amendment is allowed to stand, roving wiretaps will begin to be issued with the same frequency as other types of electronic surveillance. Given the leeway that a roving wiretap gives law enforcement officers, this result cannot be allowed to come to fruition. Therefore, it is imperative that courts find the amended roving wiretap statute unconstitutional, thereby requiring Congress to replace the newly added "could have" requirement with the original "purpose" requirement.

V. CONCLUSION

"By its very nature eavesdropping involves an intrusion on privacy that is broad in scope."[172] The roving wiretap statute, as originally enacted, gave federal investigators a potent weapon in their effort to intercept the communications of suspected criminals. However, the statute contained significant safeguards that limited the potential for abuse. Of these safeguards, the requirement that law enforcement officials demonstrate that the suspect was purposely seeking to thwart interception by changing facilities was the most significant, and in the "legislative dead of night,"[173] this requirement was eliminated.

The amended version of the roving wiretap statute replaces the "purpose" requirement with a standard that is too transparent—the "could have" standard. Courts must find that the amended statute is unconstitutional because it violates the Fourth Amendment, thereby forcing Congress to put the "purpose" requirement back into the statute. Only with the "purpose" requirement can the roving wiretap statute meet the particularity requirement of the Fourth Amendment.

& MCKENNA, *supra* note 20, at §§ 14:1 to 14:23.

Minimization will not effectively reduce the number of innocent conversations that are intercepted because of the deference to investigators in showing that they acted in "good-faith" when following minimization guidelines. *See id.* § 14:4 (explaining that the Supreme Court has been very deferential to the government when questions of minimization arise).

[170] *See supra* notes 97–100 and accompanying text.

[171] *See supra* note 75, at H9731 (statement of Rep. McCollum) (explaining that roving wiretaps were too difficult to obtain).

[172] Berger v. New York, 388 U.S. 41, 56 (1967).

[173] *See* Gillmor, *supra* note 67, at 1C.